Maryland
DEPARTMENT OF HEALTH
Larry Hogan, Governor · Boyd K. Rutherford, Lt. Governor · Dennis R. Schrader, Secretary

January 12, 2022

On December 4, 2021, the Maryland Department of Health (MDH) experienced a security incident involving its information technology system. There is no evidence at this time that this incident resulted in unauthorized access to, or acquisition of, any data.

The state's Unified Incident Command continues its ongoing response and the focus remains on three main areas: protecting the MDH network, restoring core services, and conducting a thorough forensic investigation into the incident.

Employees are to report to their respective MDH offices as scheduled or directed by their manager. As part of our ongoing efforts to protect the MDH network, employees may only use state issued laptops or desktops specifically cleared by the Office of Enterprise Technology (OET). Employees may use devices issued after December 6, 2021.

The following frequently asked questions (FAQ) are updated. If you have any additional questions, please submit them here. We greatly appreciate your patience while we continue to thoroughly assess and restore impacted systems.

FREQUENTLY ASKED QUESTIONS

1. **Which MDH / systems and offices are impacted?**

   The security incident impacted multiple MDH-hosted systems and offices. Our teams and partners are working nearly around the clock to ensure that systems supporting health and human safety functions are prioritized for assessment and restoration.

2. **Why can't I use my state issued device?**

   All MDH devices (laptops and desktops) are part of the overall investigative process and must remain in their current state until cleared by the forensic investigation and restoration teams.

3. **What MDH devices are authorized for MDH employees and contractors to use and are there restrictions?**

    - Employees may only use state issued laptops or desktops that have been cleared for use by OET. Unless state issued laptops or desktops have been cleared for use by OET, or an employee has been issued a new laptop or desktop, employees must not use MDH-issued laptops and desktop computers.
    - Employees reporting on site should not log into their computers. MDH issued cell phones can continue to be utilized via cellular service only.
    - MDH WiFi service should not be utilized.
    - MDH issued MiFi devices can continue to be utilized to connect personal laptops to the internet (cellular data only).
    - No MDH data can be downloaded or created on software that is installed on personal devices such as Word or Excel. Documents can be created in Google Docs or Sheets as they are cloud based
    - Any tablets (iPads, Androids) are considered mobile devices and cleared for use. Domain joined tablets like the Surface Pro are **not approved** for use and should follow the guidance for laptop and desktops.
    - Docking stations that have no desktop/laptop currently connected can be unplugged and used.
    - Printers/scanners/copiers connected via USB or network (201 W. Preston Street network excluded) are permitted to be redeployed for use and must NOT have any connectivity to the impacted MDH network in any way.
    - See the attached MDH Teleworking InfoSecurity Requirements.

4. **What services can be used?**

    - Accessing Amazon Workspace from OET cleared MDH devices is allowed.
    - Accessing Google Workspace from non-MDH devices is allowed.
    - Telework staff may access Google Services from a non-MDH device using home internet access, or MDH cellular or hot-spot data only.
    - If accessing Google Workspace from a personal device, all files are to remain in Gmail or Google Drive; downloading of files to personal computers is prohibited.

5. **When can I use my MDH laptop that is currently turned off?**

    - Do not power on or use any unauthorized device unless directed by OET or the Restoration Team.
    - Directions will be provided by OET or the Restoration Team Project Manager regarding the next steps for laptops or desktops that were involved in the security incident.

6. **Should MDH staff come into the office?**

    - Employees should continue to report to MDH offices according to the direction of their managers. MDH offices continue to be open and operational to support clients and constituents. Employees will be assigned a work location based on where they are able to perform work functions.
    - On December 10, 2021, MDH established a “hoteling space” with 58 laptops, internet connectivity, and printer capability at 301 W. Preston Street in the space formerly used as the cafeteria. Staff may request to work from that location when necessary or managers may assign staff to that location when necessary in order to complete required work assignments. Personal devices are not required to be used at the 301 W. Preston hoteling location.
    - Due to the increase in COVID-19 cases, precaution measures have been taken at the hoteling location, including socially distancing the work stations and cleaning equipment between each use.
    - MDH is also working with sister agencies who have available space and access for MDH staff to report and complete work assignments. Managers will work directly with staff as necessary in these situations.
    - When staff are directed to report to a workplace other than their regularly assigned worksite or their telework location, applicable policies and procedures for work-related travel will be used.

7. **How can staff telework? What are the telework requirements?**

    - Staff whose assigned work can be completed via telework may be approved by their manager to do so, provided the staff are willing to use their personal laptop/desktop, internet access, and other devices. Personal computers should not be used to save or store any information that is considered protected health information (PHI) or personal identifiable information (PII).
    - Staff whose assigned work can be completed via telework, but who are not able/willing to use personal equipment, should report to the workplace.
    - Staff whose assigned work cannot be completed via telework should report to their workplace, as assigned by their manager.
    - In situations where in-person coverage is required at a work location, staff (telework eligible or not) may be directed by their supervisor to report to the workplace. Management should make such assignments in order to maintain the highest level of effective and efficient service delivery, while distributing responsibilities across staff as evenly as possible.
    - If staff assigned to an MDH worksite are able to complete some of their regularly assigned duties through the use of their personal device while onsite, they may do so. If warranted, managers may request a loaner device for these situations according to the request and prioritization process as established by OET.

- If accessing Google Workspace from a personal device, all files are to remain in Gmail or Google Drive; downloading of files to personal computers is prohibited.
- All security related requirements for Teleworking can be found in the MDH Teleworking Info Security Requirements

8. **Can employees be directed to work from personal devices or take leave?**

    - Employees who do not have an assigned IT device and choose not to use their personal computers, in order to telework as offered, should report to their assigned work location. Managers may choose to have employees report to the hoteling space as an assigned work location.
    - If an employee requests to use their accrued leave, managers should consider the request and approve or deny based upon operational need and the type of leave being requested. Administrative leave is not being granted.

9. **What is the timeline for this situation to be resolved?**

    MDH continues to thoroughly assess critical systems involved in the security incident and is identifying processes needed to support restoration. This is a time consuming process as the incident affected multiple network systems. MDH will keep employees updated as more information becomes available.

10. **Can MDH issued cell phones be used?**

    Yes. Cellular data must be used, however. Cell phones should not be connected to MDH WiFi.

11. **What should MDH programs do if they are unable to function without network access? What if the program is a public service and can't be shut down?**

    Programs and Business units should document the impacted systems or services using the Network Status Form previously submitted and engage with their IT Management and OET to begin work around and prioritization discussions.

12. **Can staff open email attachments?**

    Yes; open in Google Drive.

13. **What should I do with my current IT equipment?**

    Hold on to all IT equipment until given further direction. If the device is on, leave it on. If the device is off, leave it off.

14. Can staff print from Google to a home printer?

Print any items from the document preview screen; shred / dispose of documents accordingly.

15. Can MDH offices edit their websites?

At this time, there are two points of contact available to support time sensitive MDH website content edit requests. We ask that you please consider the urgency of your content updates and limit those updates to those that are most imperative. You may request content updates by the following methods:

1. Submit a ticket here.
2. Contact the OET Help Desk during business hours at 410-767-6534.

16. Can Performance Evaluation Program (PEP) forms be made available on Google Forms? These previously could be downloaded from the DBM website.

These forms are still available on the DBM website.

17. What do I do if I receive an email I don't recognize?

Due to this security incident, there has been an increase in spam and phishing attempts using the situation as "bait" to trick individuals into clicking on malicious links. If you do not recognize the sender of an email please follow the phishing report process by clicking on the "3 dots" in the upper right of the email, click and then select "Report Phishing". If it was a text message you received on your device, you can simply delete it and if you continue to get the messages you can block the Sender in your phone. If the issue continues after these steps, please contact mdh.cybersecurity@maryland.gov.

18. Has the security incident impacted Workday?

No. Login into Workday here. In addition, DBM's website provides information on accessing Workday and the HUB. The link is here. If any employee has additional Workday questions, but do not know their assigned HR representative, they may call 410-767-6403 for assistance.

19. Is the Job Apps system on-line?

- The JobAps system, used for recruitments and hires, remains functional. However, the number of users with access is reduced. OHR Recruitment team is supporting the recruitment efforts at healthcare facilities, local health departments, and headquarters units so that jobs will continue to be posted and applications will continue to be reviewed.

- Due to the Security Incident and our inability to use work computers, a limited number of MDH employees will be able to access JobAps to review applications or enter hire details until the MDH network system is restored.
- If you have pending hires or recruitments that need processing, please forward all hire information to your Recruitment HR Officer and/or hiring manager as you normally would.

20. Is the OET Helpdesk active?

Yes, the OET help desk is active and can be reached at 410-767-6534.

21. What should I do if someone from the media contacts me?

Refer all media inquiries to MDH Deputy Director for Media Relations, Mr. Andy Owen, andy.owen@maryland.gov.

If you still have questions, please direct them to your supervisor.